Beginning a new PSS design

Presentation to TWG
March 20, 2003

John Carwardine
Roy Emerson
ASD Electrical Systems Group

Why another design cycle?

- Current PLC hardware will be obsolete before we finish building beamlines.
- “Version-1” PSS cannot support some of the upcoming beamline designs.
- Address reliability issues, e.g. avoid having to disconnect field wiring during validations.
- Desire to automate parts of the validation process for speed and effectiveness.
- Desire for better self-diagnostics to speed troubleshooting and repair.
- New design will build on our experience with the existing systems.

Key Requirements

- Meet the safety and operational needs of the beamlines in a cost-effective manner.
- Support APS and beamline reliability & availability goals. *[Operational transparency]*
- Should not be unnecessarily complicated to operate or support.
- Standardized hardware and software to simplify support and maintenance.
- Accommodate all known and anticipated beamline configurations.
- Support non-invasive PSS validations.
- Facilitate shorter validation times.
- Provide automated self-test and self-diagnostic capabilities.
- Should be possible to retrofit key benefits into existing PSS systems.

PERSONNEL SAFETY SYSTEM

PSS Version 3 Review and Evaluation

by

Roy Emerson (ASD)

March 20, 2003

ADVANCED PHOTON SOURCE
ACCELERATOR SYSTEMS DIVISION

PERSONNEL SAFETY SYSTEM

AGENDA

- Scope
- Purpose
- PSS Design Criteria
- PSS Design
- PSS Operating Experience
- Lessons Learned
- PSS New Design Requirements
- Conclusions

PERSONNEL SAFETY SYSTEM

SCOPE

The scope of this presentation is to receive input from interested parties of recommendations for changes to the PSS.

Issues to be considered in this review

- Chain-A and Chain-B processors and associated field equipment.
- FERDP and associated field equipment
- PLC remote I/O and associated field equipment.
- ***User control interfaces***
- ***User Interfaces (Remote shutter operation, EPICS, possibly others).***
- DI water interfaces to PSS.
- Who's responsible for developing the software (HIL) simulator for Version 3 ?

Does not include

- Field devices such as door switches, speakers, crash buttons, limit switches …
  The devices and requirements for Version-1 systems will apply.
- Pneumatic controls for front-end or beamline shutters or for station doors.

PERSONNEL SAFETY SYSTEM

PURPOSE

The purpose of this presentation is to demonstrate important lessons learned during the past six years of PSS operation and then utilize this information to produce a more dependable PSS by partitioning its functionality differently while maintain compliance with existing safety criteria.

PERSONNEL SAFETY SYSTEM

PSS Design - Versions 1 and 2

- The APS Personnel Safety System (PSS) is a high reliability, fail-safe, redundant, engineered safety system to monitor and control personnel access into potentially hazardous experimental stations and inhibit or mitigate the prompt radiation hazard to personnel.

- Each beamline PSS is designed by the APS/ASD/ES-ISIG staff to meet the following requirements: safety envelope defined by DOE Order 420.2, APS SAD, and individual CAT requests after internal review.

- The current PSS design has both command/human machine interface (HMI) and emergency shutdown (ESD) functionality in Chain-A and ESD functionality in Chain-B. DOE (Guidance Part I.F.b.4.b) requires only interlock function.

- EPICS handles PSS maintenance warnings and alarms for both Chains.

PERSONNEL SAFETY SYSTEM

PSS Design Criteria

If the answer is yes for either of the following questions the corresponding signal must be connected to the Emergency Shut Down (ESD) portion of the PSS

1. Does this signal (assertion, negation, or loss of) indicate a need to immediately shutdown the beam to "prevent exposure of personnel in excess of the most current DOE standards for ionizing and non-ionizing radiation" DOE 420.2 par. 9.c.(1)

2. Does this signal
   a. permit the operation of a critical device as defined by DOE G 420.2 part 1.F. par. 2.b.(4) and require implementation by dual chain as set forth in SAD 3.11.1.3.2.5 or disable the storage ring under conditions set forth in SAD 3.11.2.1
   b. monitor a critical device as required by DOE G 420.2 part 1.F.par.2.b.(4)(b)
   c. or indicate that said device is not operating within normal conditions. An example of operation exceeding normal conditions and the need for protection is given in DOE G 420.2 part 1.D. par. 3.d.

PERSONNEL SAFETY SYSTEM

PSS Design Criteria Compliance with DOE 420.2

1.F.2.b Technical Design

(1) Fail Safe design

All protective functions are designed for fail-safe operation.
Unsafe conditions require energized complete circuits.

(2) No single point failure

All critical devices are duplicated in each chain.

(3) Component protection

All PSS wiring and systems in dedicated racks, cable trays, and armored conduit.

(4).(a) Redundant critical devices

All critical devices have a backup

(4).(b) Redundant status of critical devices

Both chains independently monitor all critical devices.

(7) Modular Design

Components of the PLC systems are of modular design for easy expansion and replacement.

(8) Testing

Each beamline can be independently taken offline for testing.

1.F.2.c Personnel Exclusion Areas

(1) Emergency shut-off devices

Crash buttons are placed in each station.
Number and placement is selected to ensure easy access.

(2) Emergency exit mechanisms

All doors are equipped with emergency egress buttons that release the door.

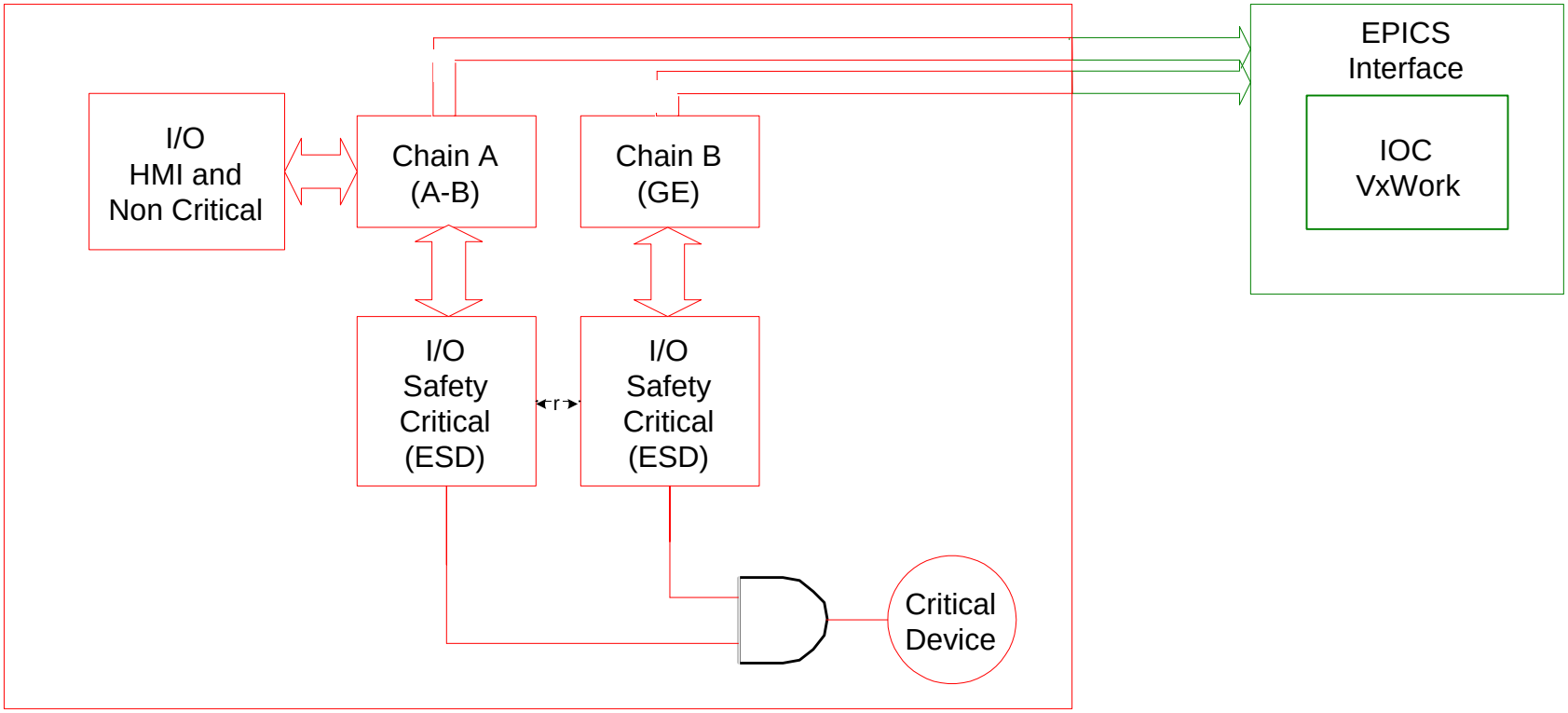
(4) Search procedures

Exclusion area searches are incorporated into the PSS.

PERSONNEL SAFETY SYSTEM

Block Diagram

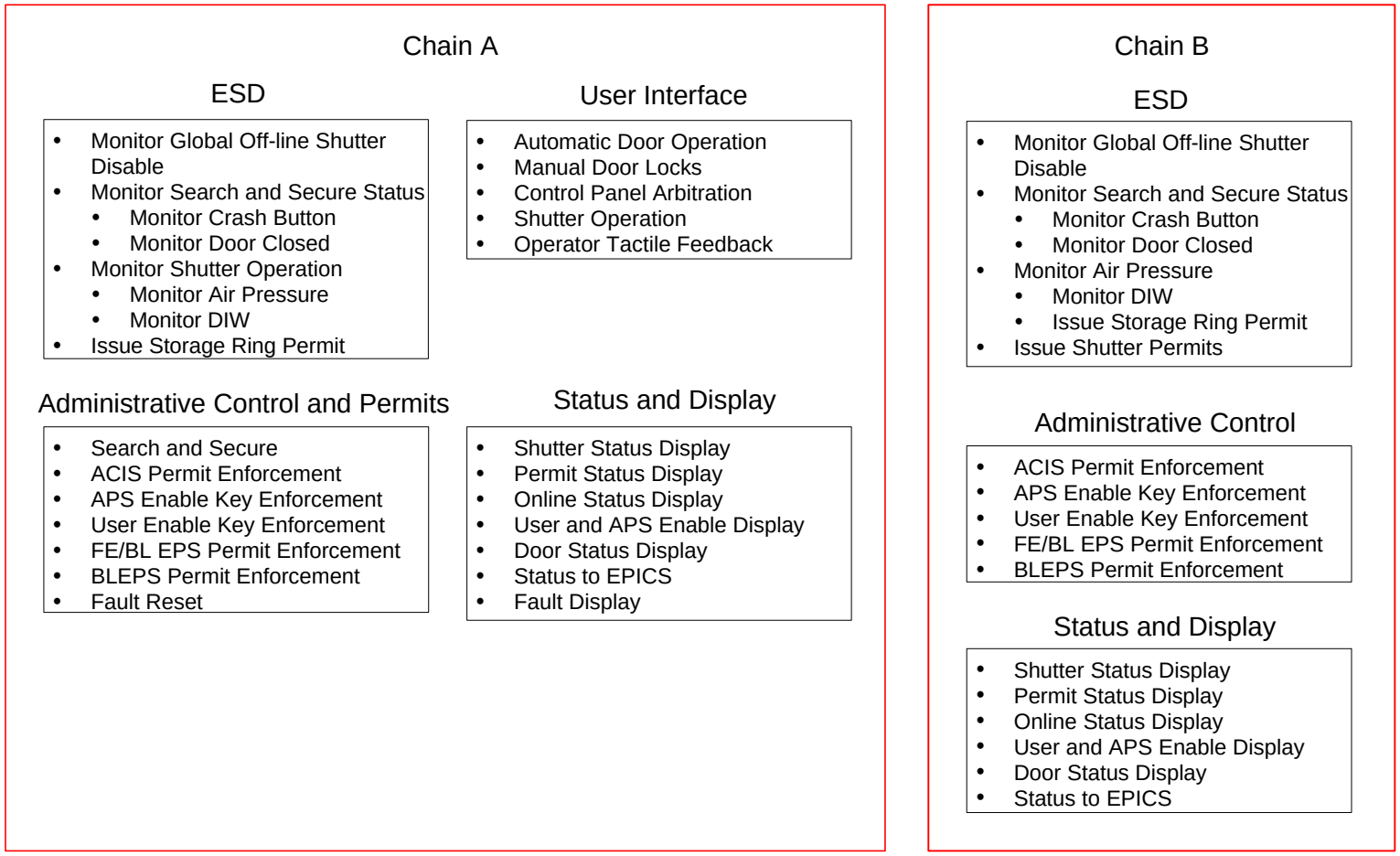
Version 1



PERSONNEL SAFETY SYSTEM

Functional Block Diagram

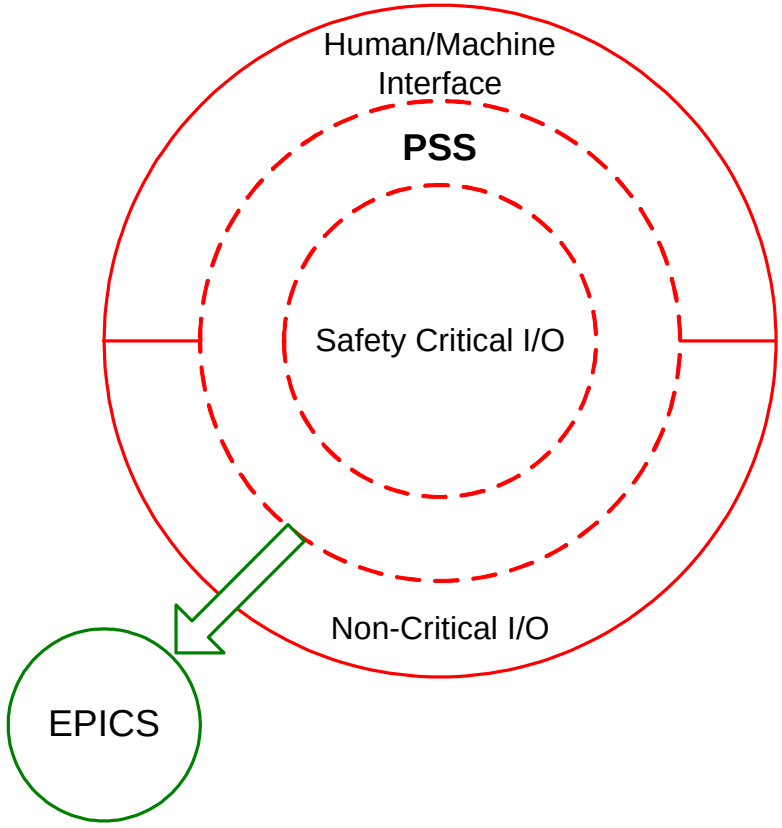
Version 1



PERSONNEL SAFETY SYSTEM

Communication Layers

Version 1



PERSONNEL SAFETY SYSTEM

PSS - Lessons Learned

Lessons Learned

- Over 95% of PSS-related User down time was due to either FE shutter opening problems or station door operation not PSS operation.
- Less than 1% of the Software Change Request (SCR) changes are to the ESD portion of code.
- Over 98% of PSS software change requests involved only HMI functionality not emergency shutdown tasks.
- PSS version 1 design has both HMI and ESD functionality in Chain A thus:
  i) changes in HMI code exposes the ESD code to unintentional modifications.
  ii) each SCR requires extensive testing be done to the entire Chain A software.
  iii) faults in Chain A resulting from uncommanded operations in chain B.

PERSONNEL SAFETY SYSTEM

PSS - Lessons Learned

Proposed Changes

- Remove all HMI and C&C functions from ESD portion of the PSS.
- Locate the HMI and C&C functionality in a third processor.

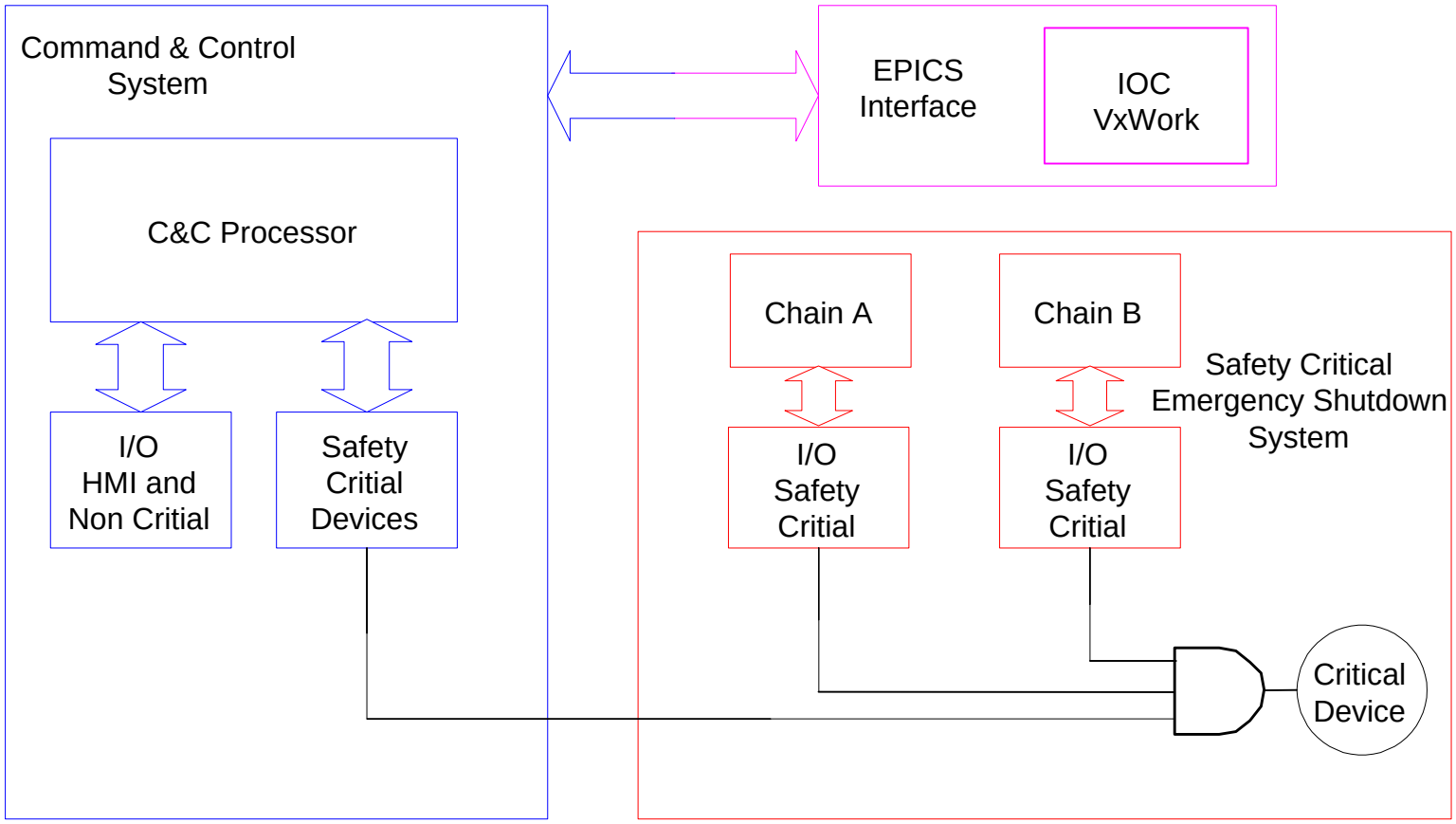
Proposed Modifications

1. ESD software Chain A and B simplified
   - More complete test coverage (exhaustive limit) of ESD code.
   - The amount of effort to validate PSS ESD functionality reduced.
   - Shorter PLC scan times > better ESD response times.
2. New functional partition reduces the risk of unintentional changes to ESD code.
3. Safety envelope functionality unchanged.
   - Employ same H/W and configuration > complies with criteria.
   - ESD functionality complies with design criteria.
   - Requirements analysis done on new design (ARM, SpecTRM, SCR).
4. Time to generate “new” non-ESD code for different CAT’s reduced
5. Provide a more programmable USER interface > math type & quantity changes.
6. C&C non PLC platform > extensive s/w tools for development, V&V and SCM

PERSONNEL SAFETY SYSTEM

Block Diagram

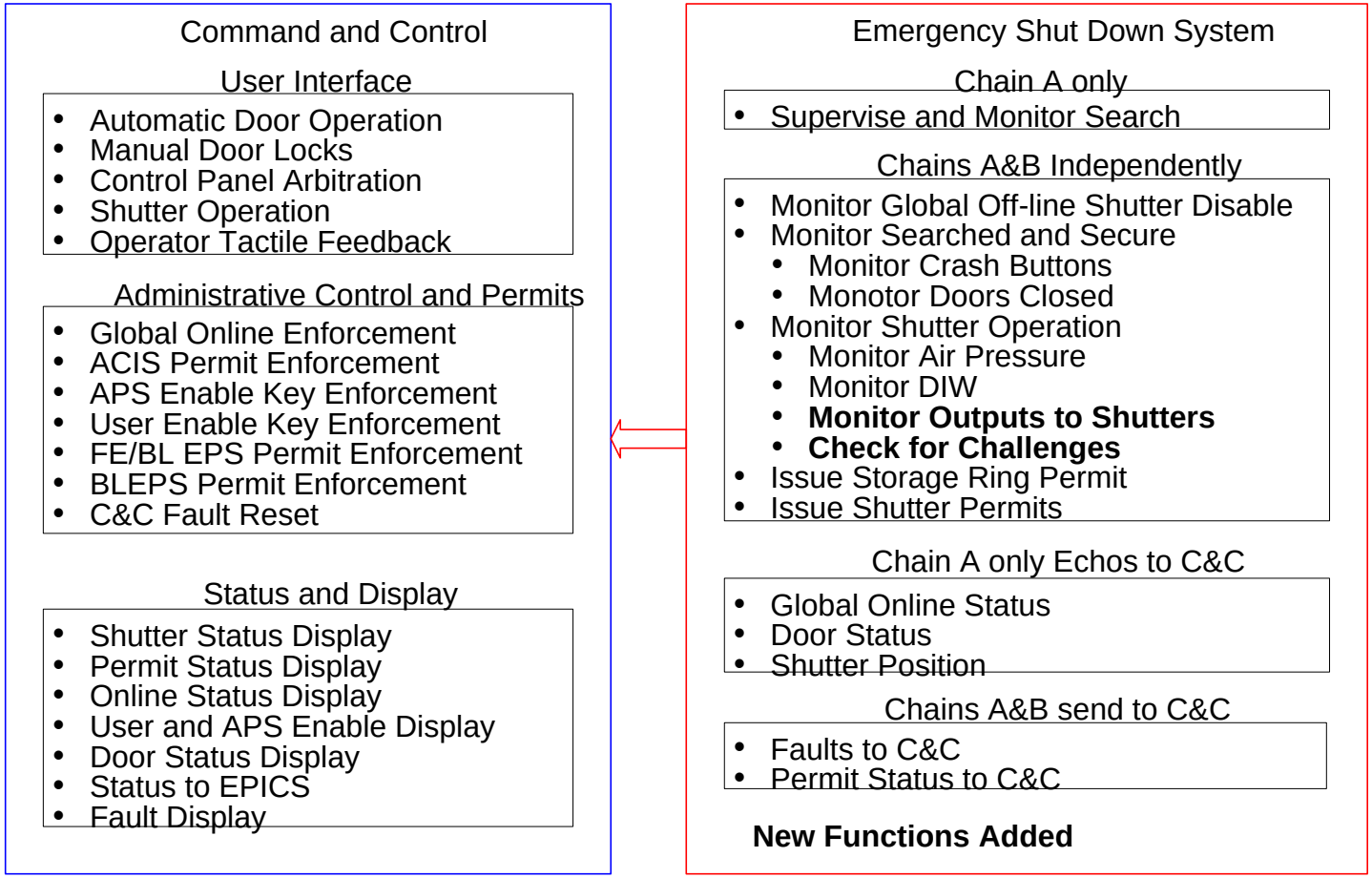
Version 2



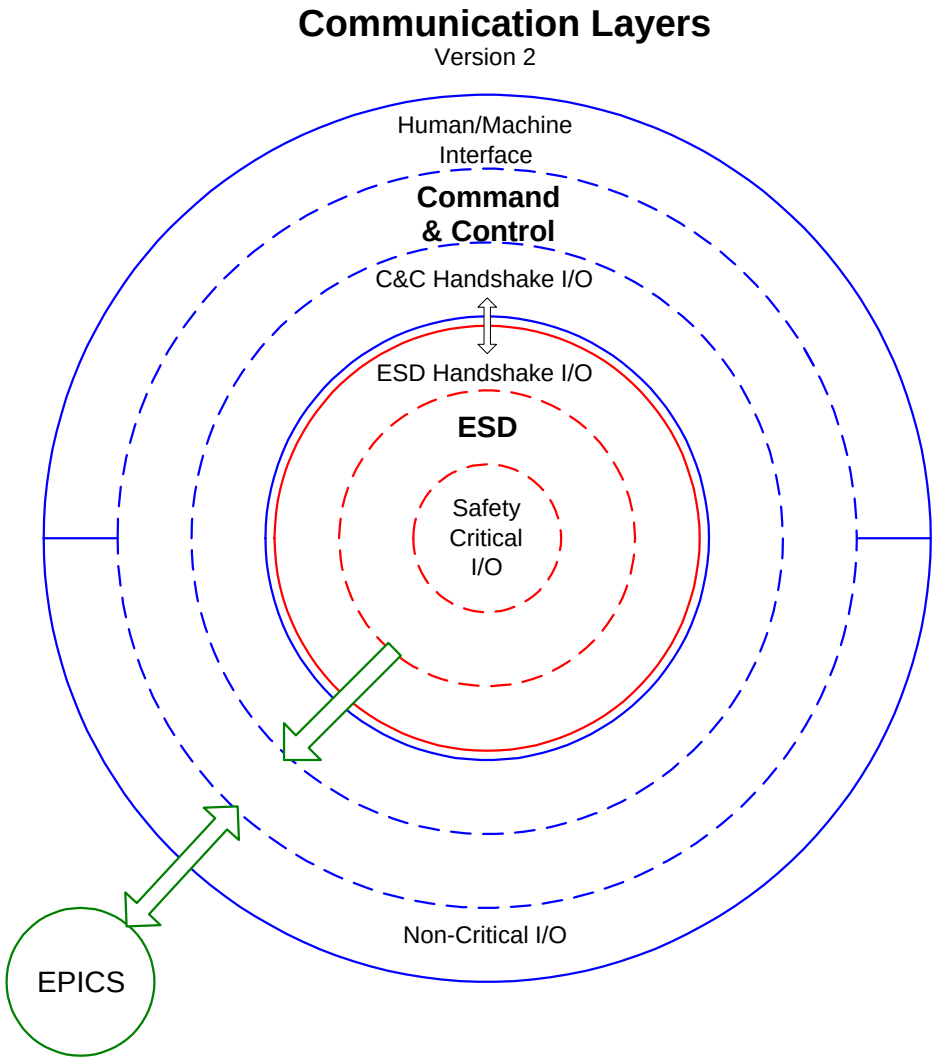
PERSONNEL SAFETY SYSTEM

Functional Block Diagram

Version 2



PERSONNEL SAFETY SYSTEM



PERSONNEL SAFETY SYSTEM

PSS Beamline Safety Envelope

Current	Version 2	
Combined	ESD	C&C
• Shutters only open when interlocks satisfied other permits controlled by chain door interlocks permits by chain	• Door interlocks are independently by both before shutter open	• Shutter only open when interlocks satisfied and permits
• Chain A verifies shutters are commanded within worst case allotmen • Both chains independently water • Both chains independently crash • Chain A only allows door unlock when shutters • Chain A supervises and searchboth chains verify status maintained while open	• Both chains independently shutters are where within worst case time • Both chains independently water • Both chains independently crash • Both chains monitor doors shutters • Both chains verify search maintained while shutters	• Verify shutters are commanded within normal allotmen • Proper water required to open • Crash buttons must be open • Only allows door open/unlock shutters • Supervises and monitors
• System detects output through monitoring of indicators i.e. limit	• System detects output through both direct outputs and secondary • Both chains can detect to interlocks by	
C&C functions embedded in		• Outputs monitored by attemped disallowed • Monitors emergency

PERSONNEL SAFETY SYSTEM

Conclusions

- Operating experience shows that APS USERS will continue to need semi-custom and dynamic PSS operational profiles (i.e. HMI) that will demand continued software changes. (Touch Screens)

- Operating experience indicates that the current mixed HMI/ESD code PSS system is safe and reliable but vulnerable. Experience has also shown that with isolated ESD and C&C code the PSS can be made simpler, more reliable, less vulnerable and considerably improve the testable.

- HMI and C&C tasks should remain a part of the non-ESD PSS to provide protection against accidental or unintentional operational challenges and to provide a reliable, standard HMI interface to the APS USERS.